IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

May 01, 2025

IN THE MATTERS OF THE SEARCHES OF: 3501 NORMANDY LANE, APT. 8 ROANOKE, VIRGINIA 24018 & INFORMATION ASSOCIATED WITH FACEBOOK ACCOUNT: **100001352749776** THAT IS STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	Case No. 7:25-mj-79 Case No. 7:25-mj-80

CLERK'S OFFICE
U.S. DISTRICT COURT
AT ROANOKE, VA
FILED
May 05, 2025
LAURA A. AUSTIN, CLERK
BY: s/ S. Neily, Deputy Clerk

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH WARRANTS

I, Aaron Kellerman, a Special Agent (SA) with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications for search warrants under Federal Rule of Criminal Procedure 41 to authorize the search of: (1) 3501 Normandy Lane, Apartment 8, Roanoke, Virginia 24018, located within the Western District of Virginia and for; (2) information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Facebook, a social media services company headquartered at 1 Meta Way, Menlo Park, CA 94025, in the Northern District of California. This Court has jurisdiction to issue the latter request because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

2. The residence to be searched is described in Attachment A-1 and the things law enforcement is requesting to seize from the residence are more particularly described herein and in Attachment B-1. The electronic information to be searched for is described below and in Attachment A-2, and I am seeking this warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B-2. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. Specifically, I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since September 2003. I received initial training and instruction to become a Special Agent at the FBI Academy located in Quantico, Virginia, which included training concerning violations of the United States criminal statutes. I am currently assigned to the Richmond Division of the FBI, Roanoke Resident Agency. I am presently and have been previously assigned to investigate a variety of criminal matters, to include violent criminal acts, gangs, and drug investigations. Further, I have experience and training in a variety of investigative and legal matters, including the topics of lawful arrests, the drafting of search warrant affidavits, and probable cause. While serving within my capacity at the FBI, I have authored search warrants concerning various federal criminal violations. I have investigated cases where electronic communications, to include social media platforms and cellular telephones, have played an integral

role in the investigations. Through experience and training received, I have become familiar with how the usage of electronic devices and social media applications has become commonplace throughout the "criminal world." I am also aware that information stored at the service provider facilities and on cellular devices themselves can assist law enforcement in criminal investigations.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary for the limited purpose of establishing probable cause to conduct a search of the residence described in Attachment A-1 and the information described in Attachment A-2 for the items and information described in Attachments B-1 and B-2 for evidence, contraband, and/or instrumentalities of the criminal conduct described herein. Additionally, unless otherwise indicated, wherever in this affidavit I assert that an individual made a statement, that statement is described in substance herein and is not intended to be a verbatim recitation of such statement. Furthermore, unless otherwise indicated, all statements contained in this affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 401 and 402 (Contempt of Court) and Title 18, United States Code Sections, 1513(e) (Retaliation Against Witnesses or Informants) and 1513(f) (Conspiracy to Retaliate Against Witnesses or Informants) have been committed. There is also probable cause to search the residence described in Attachment A-1, and the information described in Attachment A-2, for evidence of a crime, contraband or other items illegally

possessed, or property used in committing a crime, as further, and respectively, described in Attachments B-1 and B-2.

PROBABLE CAUSE

7. On February 24, 2021, a federal grand jury returned a five-count Superseding Indictment against Jordan Tyree Bondhill, Aaron Tysean Cotton, and Jayquan Shameek Andrews (ANDREWS), alleging in Count Five (hereinafter the "conspiracy count") that beginning in or about August 2019 and continuing until in or about September 2020, the three defendants conspired to possess with intent to distribute, and to distribute, 50 grams or more of pure methamphetamine and 500 grams or more of a mixture and substance containing a detectable amount of methamphetamine, all in violation of Title 21, United States Code, Sections 846 and 841(a)(1) and (b)(1)(A). *See United States v. Jayquan Andrews*, Case No. 7:20-CR-00076.[1]

8. Prior to their arrests, Bondhill, Cotton, and ANDREWS had been identified by law enforcement as members of a local neighborhood gang set, who were involved in committing narcotics, firearms, and violent crimes in the City of Roanoke, Virginia. During their investigation into this group, law enforcement also learned that its members actively utilized Facebook, to include posting messages to the public or their friend groups boasting of their "gang" affiliation and, on occasion, communicating with one another about their criminal activities.

9. [redacted]

[1] On January 25, 2022, a Second Superseding Indictment was filed, naming ANDREWS as a defendant in two additional counts, alleging that he distributed a mixture and substance containing a detectable amount of cocaine on two different occasions, in violation of Title 21, United States Code, Section 841(a)(1) and (b)(1)(C).

[redacted]

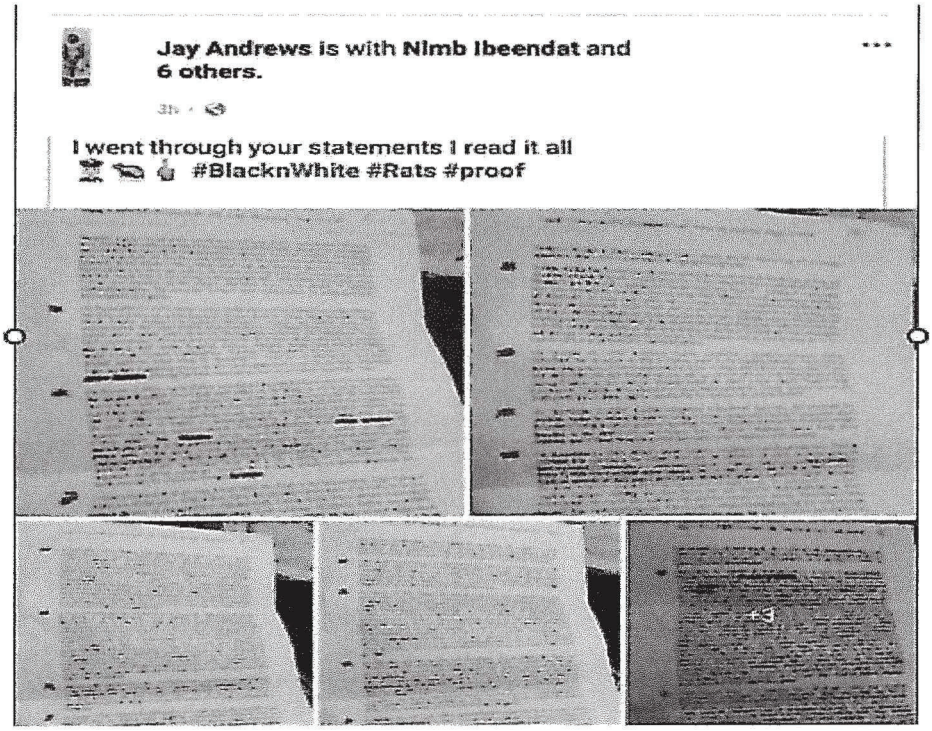
10. Based upon the evidence uncovered during law enforcement's investigation into the group, [redacted] ANDREWS pleaded guilty to the conspiracy count and [redacted] sentenced to 120 months imprisonment. Prior to [redacted] sentencing hearings, as is customary, the Probation Office filed a Presentence Investigation (PSR). As it relates to the requests made herein, I will focus on the Final PSR filed in ANDREWS'S case.

11. On September 26, 2022, the Probation Officer filed the Final PSR in ANDREWS'S case. The ECF number associated with this filing was 188, and the report was 38 pages long. In this report, [redacted] were statements made by [redacted] cooperating witnesses. Importantly, the cover page of the PSR reads as follows:

> **The contents of this report are confidential and restricted to the defendant, the defendant's attorney, and an attorney for the government. Standing Order No. 2015-8, entered on January 8, 2016, prohibits a defendant who is incarcerated from possessing a copy of the report while in custody unless given permission from the Court.**

12. Standing Order No. 2015-8, affixed hereto as Attachment C, further describes the circumstances upon which an incarcerated defendant may possess a copy of their PSR. To my knowledge, ANDREWS, who was brought into federal custody on January 25, 2021, and was sentenced on October 3, 2022, has remained in continuous custody since his arrest. I am also not aware of ANDREWS receiving permission from the Court to possess his PSR or otherwise disseminate it to other individuals for his own safekeeping.

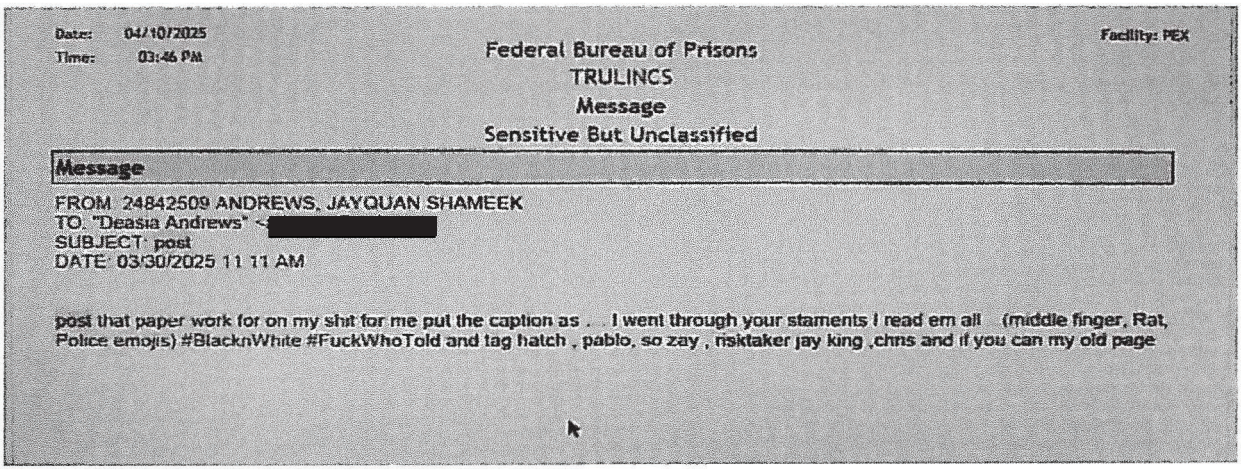
13. On or about April 2, 2025, the FBI learned of a Facebook post containing images of several pages from ANDREWS'S Final PSR, identifiable by its ECF number and pagination. Specifically, these images related to portions of the PSR that included statements made to law enforcement by cooperating witnesses, [redacted] The posts were made by someone utilizing the screen name "Jay Andrews" (Facebook ID 100001352749776), and the picture associated with the profile, although difficult to see in the image below, is a picture of ANDREWS.



14. While the name of one individual, [redacted] was "redacted," the names of cooperating witnesses and other individuals who supplied information to law enforcement implicating ANDREWS, and other members of his group, could be observed in the images. Multiple individuals, including Bondhill ("Pablo Bills"), were "tagged" in the post and in response to a comment that read "That's what you supposed to did brabra. Produce the Proof 100 100," "Jay Andrews" replied, "facts bra shit got me 10 years." While the post has since been taken down, as of the evening of April 2, 2025, the post had been "liked" 214 times, commented on 25 times, and reposted 103 times.

15. At the time this post was made, ANDREWS was incarcerated at Federal Correctional Institute (FCI) Petersburg Medium in Petersburg, Virginia. BOP advised that ANDREWS would not have a legitimate way to access Facebook based on the conditions of his confinement. After the FBI alerted BOP to his possible possession of contraband (the PSR and perhaps a cellphone that potentially could have been used to post the PSR on Facebook), BOP employees searched ANDREWS'S cell, but did not find a copy of the PSR or a cellphone.

16. BOP later provided the FBI with copies of ANDREWS'S emails and recorded phone calls. In reviewing this information, I found the following communication between ANDREWS and his sister, Deasia Andrews (DEASIA):



Date: 04/10/2025
Time: 03:46 PM

Federal Bureau of Prisons
TRULINCS
Message
Sensitive But Unclassified

Facility: PEX

Message

FROM 24842509 ANDREWS, JAYQUAN SHAMEEK
TO "Deasia Andrews" <[redacted]
SUBJECT post
DATE 03/30/2025 11 11 AM

post that paper work for on my shit for me put the caption as . I went through your staments I read em all (middle finger, Rat, Police emojis) #BlacknWhite #FuckWhoTold and tag hatch , pablo, so zay , risktaker jay king ,chris and if you can my old page

17. ANDREWS sent this message to his sister approximately three days before the Facebook post, and ANDREWS'S instructions for what to post closely match what was actually posted on his Facebook page. During a recorded jail call to DEASIA on April 8, 2025, ANDREWS, in an apparent reference to the post, stated that he "post that shit because I'm exposing these rats." Additionally, in reviewing the images of the PSR on the post, it appears that the pages are folded in a manner that suggests the PSR was mailed.

18. A search of Virginia Department of Motor Vehicle (DMV) records on or about April 21, 2025, revealed an active license for DEASIA at 3501 Normandy Lane, Apt. 8, Roanoke, Virginia 24018 (the TARGET RESIDENCE). During surveillance conducted on or about April 22, 2025, law enforcement observed a black female, who appeared to match the description of DEASIA, entering and driving a black Dodge Avenger parked in spot 8 outside of 3501 Normandy Lane. On or about April 28, 2025, the management at the apartment complex confirmed that DEASIA was the only individual on the lease at 3501 Normandy Lane, Apt. 8, and that the spot marked 8 was reserved for the occupants of that unit.

19. Based upon the foregoing, it appears that Deasia posted the PSR on Facebook at ANDREWS'S request and that she resides at the TARGET RESIDENCE. Based upon my training and experience, I know that individuals maintain documents inside their residence and that the more important the document (for example, legal documents), the more likely it is to remain stored inside a residence for a longer period of time. Additionally, in my review of the information provided by BOP, to date, I have not found any communications between ANDREWS and his sister discussing the destruction or disposal of the PSR. Therefore, I submit there is probable cause to believe that ANDREWS'S PSR is located within this residence.

20. Further, and as discussed below, I know in order to post something on Facebook, an individual must utilize an electronic device, usually a computer, iPad, or a cell phone. Based upon my training and experience I am also aware that individuals possess these devices in their residence. Therefore, I submit that there is probable cause to believe that DEASIA not only used an electronic device to make this post, but that the device she used will be located inside her residence and will contain evidence related to her posting the PSR at ANDREWS'S direction. Therefore, I also seek permission to seize and search any such devices found inside her residence in order to confirm that DEASIA made the post, and what, if any, conversations she may have had with ANDREWS, or others, relating to the PSR, how it came into her possession, and the post itself.

21. In seeking the Court's permission to seize and search DEASIA'S electronic devices, I also believe that potential evidence related to ANDREWS'S intent in making the post may be discovered. While law enforcement is not aware of any "direct" threats of bodily harm to an individual having been made in conjunction with this post, at least one individual who was "outed," called law enforcement and expressed concern for his/her safety.[2] Additionally, [redacted] Based upon my training and experience, and law enforcement's knowledge of ANDREWS and his associates, witness intimidation and retaliation are common tactics utilized by this group, and violent criminals in general. In fact, the FBI investigated a case involving associates of ANDREWS who shot an

[2] I have tried to reach out to this individual since learning of their call, but have not received any answer and their voicemail has been full.

individual who they believed to be a "snitch," but, in fact, had not cooperated with law enforcement.

22. Title 18, United States Code, Section 1513(e) makes it a crime to "knowingly, with the intent to retaliate, take[] any action harmful to any person, including interference with lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense[.]" Given that ANDREWS sought the assistance of another in publicly posting confidential information pertaining to people who cooperated with law enforcement, whom he desired to brand as "rats," and that DEASIA subsequently complied with this request, likely knowing of its intended effect, I submit that there is also probable cause to also search DEASIA'S electronic devices, and the information sought herein from Facebook, for evidence of ANDREWS'S intent in asking his sister to post his PSR and whether DEASIA shared in that intent.

TECHNICAL BACKGROUND ON FACEBOOK

23. Meta owns and operates Facebook, a free-access social networking website that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

24. Meta asks Facebook users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account and can choose a username.

25. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

26. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

27. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or

her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

28. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can "tag" other users in a photo or video, and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

29. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats. of the date of each call. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

30. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

31. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

32. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

33. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the

account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

34. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

35. In addition to the applications described above, Meta provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

36. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

37. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event, or tags a post with a location.

38. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

39. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or

consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

40. A preservation request for the Facebook Account with the Facebook ID of **100001352749776**, was sent to, and acknowledged by, Meta on April 3, 2025. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

BACKGROUND ON COMPUTERS AND DIGITAL DEVICES

41. I submit that if a computer or digital device[3], including a wireless cellular telephone, and/or storage media are discovered at the TARGET RESIDENCE, there is probable cause to believe records or communications will be stored on those computers, devices, phones, and storage media, for the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used

[3] The term "digital device" is more fully defined in Attachment B-1.

by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

42. *Forensic Evidence*. As further described in Attachment B-1, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant but also for forensic electronic evidence that establishes how the computers and electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer, electronic device, digital device, cell phone, or storage media found in the TARGET RESIDENCE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed,

thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or

consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

43. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises.

However, taking the storage media off-site and reviewing in a controlled environment will allow examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

44. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Request to Use Biometric Features to Unlock a Locked Device

45. The warrant I am applying for would also permit law enforcement to obtain from DEASIA (but not any other individuals present at the TARGET RESIDENCE at the time of the execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) necessary to unlock any devices subject to search and seizure for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the devices. I seek this authority based upon the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to

unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or

password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the searches authorized by these warrants.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

46. Due to the foregoing, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned

biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the Device(s) found at the TARGET RESIDENCE; (2) hold the device(s) found at the TARGET RESIDENCE, in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the device(s) found at the TARGET RESIDENCE, in front of the face of the aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

47. The proposed warrant does not authorize law enforcement to require that the aforementioned person state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person for the password to any devices, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any devices, the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION

48. Based on the foregoing, I request that the Court issue the proposed search warrants.

49. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of the search warrant related to Facebook. The government will execute this warrant by serving it on Meta.

Respectfully submitted,

Aaron Kellerman
Special Agent
Federal Bureau of Investigation

Attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) on this 1st day of May 2025

HONORABLE C. KAILANI MEMMER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to Be Searched

The property to be searched, the TARGET RESIDENCE, is the residence, curtilage, and vehicles located at 3501 Normandy Lane, Apt. 8, Roanoke, Virginia 24018. The following is a picture of the TARGET RESIDENCE.

ATTACHMENT A-2

Property to Be Searched

This warrant applies to information associated with Facebook user ID: **100001352749776**, that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B-1

7-25-mj-79

Particular Things to be Seized

1. The items to be seized are evidence of a crime, contraband or other items illegally possessed, and property used in committing a crime, to wit: Contempt of Court, in violation of Title 18, United States Code, Sections 401 and 402, and Retaliation Against Witnesses, in violation of Title 18, United States Code, Sections 1513(e) and 1513(f), involving Jayquan Shameek ANDREWS and DEASIA Andrews, including:

a. Any Presentence Report of Investigation and copies thereof;

b. Any envelope or packaging that was used to mail any Presentence Report of Investigation to ANDREWS or DEASIA.

c. Computers, digital devices (including cell phones), and electronic storage media including all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers. A "storage medium" for purpose of the warrant is any physical object upon which computer data can be recorded. Examples include, but are not limited to, external hard drives, CDs, DVDs, and flash drives

d. Documentation regarding passwords to computers, digital devices (including cell phones), electronic storage media, or any passwords to programs, including those used to exchange virtual currency or other financial programs.

e. Any and all records or other items which are evidence of ownership or use of computer equipment found in the subject premises, including, but not limited to, sales receipts, bills for internet access, handwritten notes, and handwritten notes in computer manuals.

f. For any computer, digital device (including cell phones), electronic storage media, or other physical object upon which computer data can be recorded (hereinafter, "Device(s)") which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described above:

i. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

ii. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);

v. evidence of the times the Device(s) was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);

vii. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);

viii. records of or information about Internet Protocol addresses used by the Device(s);

ix. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "digital devices" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

This warrant authorizes a search of computers, digital devices (to include cell phones), electronic storage media, and electronically stored information seized or copied pursuant to this warrant in order to locate and, if discovered, seize evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

2. During the execution of the search of 3501 Normandy Lane, Apt. 8, Roanoke, Virginia 24018 (TARGET RESIDENCE), described in Attachment A-1, law enforcement personnel are also specifically authorized to obtain from DEASIA Andrews (but not any other individuals present at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Devices requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the Devices, to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

(a) any of the Devices found at the TARGET RESIDENCE;

(b) where the Devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offenses as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the Devices' security features in order to search the contents as authorized by this warrant.

3. While attempting to unlock Devices by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Devices. Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person is permitted. To avoid confusion on that point, if agents in executing the warrant ask the aforementioned person for the password to any Devices, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Devices, the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

ATTACHMENT B-2 7-25-mj-80

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Meta regardless of whether such information is located within or outside of the United States, including any messages, e-mails, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on April 3, 2025 (Facebook case number 9414797), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities from 3/1/2025 to present date;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from 3/1/2025 to present date, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which

the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and contents of communications and messages made or received by the user from 3/1/2025 to present, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the account;

(l) All records of Facebook searches performed by the account from 3/1/2025 to present date;

(m) The types of service utilized by the user;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of Contempt of Court, in violation of Title 18, United States Code, Sections 401 and 402, and Retaliation Against Witnesses, in violation of Title 18, United States Code, Sections 1513(e) and 1513(f), involving the account identified in Attachment A-2, including information pertaining to the following matters:

a. Communications related to any Presentence Report of Investigation and knowledge regarding the prohibitions against possessing and disseminating copies of a Presentence Report of Investigation;

b. Images of any Presentence Report of Investigation or discovery from ANDREWS'S criminal case.

c. Communications regarding threats, intimidation, tampering and violence against witnesses involved in ANDREWS'S criminal case or any other communications or images related to violations of 18 U.S.C. 1513(e).

d. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, a[redacted] events relating to the crimes under investigation and to the Facebook account owner;

e. Evidence indicating the Facebook account owner's state of mind as it relates to the crimes under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

g. The identity of the person(s) who communicated with the user ID about the criminal violations referenced above.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT C

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN RE: PRESENTENCE REPORTS) **Standing Order No. 2015-8**

In criminal cases in this district, a presentence report, or any copies or excerpts thereof, must not be provided to a defendant who is incarcerated, either before or after sentencing. A defendant's presentence report may be read by the incarcerated defendant in the presence of defendant's counsel, or an associate or representative of defendant's counsel, but must not be left at the facility for the defendant's review without prior permission of the court for good cause shown. Without such permission, incarcerated defendants are not to have possession of the presentence report.

The purpose of this order is to insure that confidential information contained in such reports does not cause harm to a defendant or others or otherwise frustrate law enforcement purposes or the court's proceedings.

ENTER: January 8, 2016

Chief United States District Judge